11 SEP 1986

MEMORANDUM FOR: OIT Group Chiefs

STAT FROM: [redacted]
Management Division, OIT

SUBJECT: Security Procedures for Personal Computers

1. The Office of Security recently published Secruity Procedures for Personal Computers. OIT commented on a draft version of this, but did not see the final version before publication. Some of the OIT input was not considered. D/OIT has discussed this with Security, who agreed to incorporate OIT input into the next revision. Therefore, please review the attached booklet thoroughly.

2. I would like your comments by **October 15.** If you feel you need more time to do a complete review, please let me know. If you have any questions, I can be reached on [redacted]
STAT STAT or [redacted]

STAT MD/OIT/[redacted] (11SEPT86)

Distribution:
Orig - Addressee
1 - MD Subject
1 - MD Chrono
1 - Registry

ROUTING AND RECORD SHEET

SUBJECT: (Optional)
Security Procedures for Personal Computers

FROM:
STAT
STAT
Management Division, OIT

EXTENSION | NO.

DATE 11 September 1986

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. C/DFG ✓ Comments attached				
2. C/GOG ✓ Comments attached				
3. C/NSG Called No Comment				
4. C/NSEG Called No Comment				
5. C/IISG No Comment				
6. C/MISG ✓ Comments attached				
7. C/ATPS				
8. C/M&CG ✓ Comments attached				
9. C/ESG				
10. C/SAD&E				
11.				
12.				
13.				
14.				
15.				

FORM 1-79 610 USE PREVIOUS EDITIONS

1 October 1986

MEMORANDUM FOR: Chief, Artificial Intelligence Staff

STAT FROM: [redacted]

SUBJECT: Comments on PC Security Procedures

1. This memo contains our comments on the Security Procedures for Personal Computers document from the Office of Security. This document is a great improvement over previous versions, and many of our earlier comments have been addressed. However, there are still several areas in which we have questions or concerns.

2. The document never defines what is meant by "Personal Computer", so there is some uncertainty as to just what machines would fall under these procedures. For example, is the Xerox 1100 (Golden Tiger) a personal computer? What about a Delta Data equipped with a disk drive? The Chromatics workstation on TADS? A standalone minicomputer?

3. Whenever the security procedures indicate that an action must be "coordinated" with or approved by some specific component, it would be helpful if the reason for coordination and the conditions under which approval is granted or denied were supplied. For example, Section IV.D indicates that all product demonstrations by vendors must be coordinated with OS/ISSD. Why? Under what circumstances might OS/ISSD deny my request to have a vendor demonstrate a product? How does coordination take place? Does it require only a phone call, or is there a form to be filled out or a memo to be written? Does coordination imply approval? These same concerns apply in Sections IV.A (acquisition of PCs), VII (changing from one PC security configuration to another), VII.C.1 (removal of unclassified-outside PCs), VIII.F (requests for PC networks), IX.B (use of summer-only employees), IX.C (use of modems), IX.E (use of classified PCs that have been outside Agency control), and XI.B.3 (service representative access to non-sanitized PCs).

4. What does it take to get a waiver from OS/ISSD (Section VI.B.1)? Why is an Agency Top Secret clearance required to have access to an unclassified PC? The document makes no distinction between access to classified PCs and unclassified PCs.

5. In discussing physical security of PCs in an uncontrolled environment (Section VI.B.2), the document states that access to all PCs must be controlled by an OS-approved access control device. The only example given is a Simplex lock. It is our understanding that a Simplex lock does not provide protection, since it is a trivial task to try all possible combinations of the lock in a short time (that is why visual contact with a vault door must be maintained at all times, even though there is a Simplex lock on the door). What other access control devices are there? Further, this section is supposed to be discussing security in an uncontrolled environment, yet seems to say that the first thing required is that the environment be controlled.

6. Section VI.B.2 also makes no distinction between classified and unclassified PCs when it requires that all media be removable, that all PCs must be turned off when unattended, and that the system be under the control of a TS-cleared person.

7. Section VI.B.3 discusses a security check sheet for each PC. This seems like a reasonable idea, but perhaps the idea should be extended to also apply to PC peripherals, such as printers and plotters. Peripherals should probably also be designated as classified or unclassified, with specific procedures for securing the classified devices.

8. The reason for a distinction between unclassified-inside and unclassified-outside use is not clear. If the systems are unclassified, why does it matter where they are used? Why is it not allowed to link the two types of machines (Section VII.C.2)? Is a PC located in an Agency facility designated unclassified-inside or -outside if it is used for accessing an external data base? If a PC is designated as unclassified-outside, can it ever be operated inside an Agency facility?

9. Section VII.C.3 mentions a log that the System Administrator must keep. What information should be in the log? How long must the log be kept after the equipment is returned? Is there a standard format to be used, or is a stack of scraps of paper sufficient?

10. Similarly, Section VIII.D references an audit trail that must be kept for accesses to a local area network. What information should be audited? What format is acceptable? How long must the trail be maintained? How often should it be reviewed?

11. The limitations on PC network security in Section VIII apply

only to non-mainframe networks. Why are mainframe networks exempt? Some of the restrictions imposed on PC networks are not currently enforced on our mainframe systems (items B, C, and E). Does item E really mean that an individual must be cleared for access to all information on the network in order to use any portion of the information on the network? If that is true, then why does the server also have to enforce compartmentation of information (item C)?

12. Physically separating classified and unclassified PCs sounds like a fine idea. However, with the space problems that the Agency is suffering through, requiring that an unclassified (or classified) PC have a room or cubicle all to itself may not be very realistic. We do not put classified safes in a separate room from unclassified file cabinets; why should we force such a strong distinction for PCs?

13. Section X.B is not very clear. It seems to state that in order to reuse media, it is necessary to sanitize the PC. Surely this is not the case. It is not clear at all what the final sentence, restricting the item to unclassified-inside PCs, means.

14. There are a few places in the document where specific utilities are mentioned that can aid in PC security. Since these parts of the document only apply to a small number of machine types, can it be assumed that the remainder of the document also only applies to those same machine types? If not, then a distinction must be made throughout the document whenever the regulation does not apply to all PCs. For example, Section X.C.2 states that an individual must use the KOPY program when writing unclassified data from a classified PC, yet the KOPY program is not available for all PCs. Further, it is not clear what products can be used with which machines. For example, the Wang PC runs DOS, so stating that a product works under DOS, and another version works on the Wang PC, would seem to imply that the DOS version in fact only works on some subset of PCs that run DOS (Section XII).

15. Section X.E and Section X.F indicate that the System Administrator must receive and retain copies of the Form 4261 when used for recording the movement of magnetic media. What does the SA do with these forms?

16. Section X.G gives the responsibility for media classification and storage to the System Administrator. Perhaps these are PC user responsibilities instead. Making the SA responsible is like having OIT responsible if AIM users inappropriately classify AIM documents, or if they leave a classified printout unsecured.

17. Item 10 of the PC Security Guideline refers to getting a PC approved by COMSEC. This is the only reference to COMSEC in the document. Should COMSEC be another one of the offices

listed in Section IV.A that must be coordinated with for acquisition of PCs?

18. The example given in item 3 of the PC Security Guideline is not very good. It appears that perhaps the columns are not aligned, or the line length of the format is longer than the width of the page, so that the end of the line shows up on the next line. As a result, part of the serial number appears under the Quantity heading. Further, all that appears under the Item heading is the brand name of the device (IBM). The item should probably be IBM PC, IBM Monitor, or IBM Printer. The Model should then be which specific PC version, monitor type, or printer type. Also, what is a PC w/TK? It would really be more benificial if there were a complete example PC Security Plan, showing the kind of information that is expected.

19. The document does not address loaner machines at all. These are machines that are not owned by the Agency, nor by employees, but are loaned to Agency components for evaluation by vendors, with the intention of returning the machines to the vendors after the evaluation period.

20. There are a few typographical errors in the document. The heading for Section VI is indented too much. There is an extra comma after (DOS) in Section X.H. Section X.I should read "Tapes and cartridges must be turned in to the ADP Control Officer", instead of "turned into". The instructions for preparing a PC Security Plan state to use the underlined headings, but there are no headings underlined (they are italicized). Finally, the use of hyphens in unclassified-inside and unclassified-outside is inconsistent (sometimes there are no hyphens).

21. This is the fourth time that we have reviewed this document. Although we have raised the same issues several times, and asked many questions, we have yet to receive any feedback at all from OS/ISSD except further versions of the document. We would hope that, even if our suggestions are not used, our concerns will be addressed in some sort of dialog.

STAT

UNCLASSIFIED

3:20 PM -- 15 October 1986

STAT Note To:

From:

Subject: Security Procedures for Personal Computers

Section X (PERSONAL COMPUTER MEDIA SECURITY), (C) states that ISSD recommends that vendor software not be returned to the vendor. ISSD needs to take a stronger stand on this issue. The statement should indicate that magnetic media will never be returned to the vendor.

Reference is made in the same section (2.) to the ISSD approved KOPY program and in Section XII (APPROVED PC SECURITY PRODUCTS) to four additional security products approved by ISSD and available through OIT Consulting Services Branch (File KO, Disk KO, Cart-KO, and MEMCLEAR). I understand that the integrity of this software is being challenged by STAT OIT but don't know the current status. This issue must be resolved prior to ISSD's endorsement of the products. Consulting Services Branch is not distributing the software until that time. Unless ISSD can ensure the integrity of these programs, they should omit any reference to them in the Security Procedures Guide.

The document contains no reference indicator (such as a version number) or date. Both of these would be helpful to the customer. ISSD has published two versions to date and there is no way for the customer to distinguish the most current version.

The use of a soft gray background with white lettering for the cover makes the lettering hard to read. The use of a darker background color would make the lettering stand out as well as the document. (I'm not sure ISSD would appreciate this kind of feedback, but I offer it anyway for what it's worth.)

The next version of the document should be edited more carefully. There are several typos. (e.g. p.3,VII,A,1 'information every processed' instead of information ever processed: p.7,XI,A "anestablished" instead of an established: p9,XIII,6,"Usersand" instead of Users and) (e.g. p.3,VII,

CC:

STAT

UNCLASSIFIED

DFG

CONFIDENTIAL

16 October 1986

MEMORANDUM FOR: [redacted] 25X1

FROM:

SUBJECT: Security Procedures for Personal Computers

Only comment from DFG regarding subject document is that it does not adequately address PC's installed in the field, both domestic and foreign, environments. Suggest that another doc (or two, doc for foreign field would have to be sterile) be produced to cover those subjects. Thanks for the opportunity to comment, ~~sorry~~ its a bit late.

[redacted] 25X1

CONFIDENTIAL

STAT DATE: September 24, 1986 12:15 PM

STAT NOTE TO:

SUBJECT: Comments on Security Procedures for Personal Computers

Kathy:

I can find nothing in this document that is objectionable from an operations view point. It certainly does however, raises some questions from the PC users point of view such as the Agencies ability to provide clearances for the numbers of maintenance personnel that will be required to service the PC's and other administrative questions such as the availability of recommended software and hardware (floppy disks, etc.) It's hard to argue with the need for this type of a document and the security practices addressed.

STAT If you have any questions, please call me on Thanks